TRANSMITTAL FORM

Attorney Docket No. **RPS920010016US1/2031P**

Re the application of: **Randall S. SPRINGFIELD et al.**

Confirmation No: **1231**

Serial No: **09/824,595**

Group Art Unit: **2135**

Filed: **April 2, 2001**

Examiner: **Gyorfi, Thomas A.**

For: **Method and System for Providing a Trusted Flash Boot Source**

ENCLOSURES *(check all that apply)*		
☐ Amendment/Reply	☐ Assignment and Recordation Cover Sheet	☐ After Allowance Communication to Group
☐ After Final	☐ Part B-Issue Fee Transmittal	☐ Notice of Appeal
☐ Information disclosure statement	☐ Letter to Draftsman	■ Appeal Brief
☐ Form 1449	☐ Drawings	☐ Status Letter
☐ (X) Copies of References	☐ Petition	■ Postcard
☐ Extension of Time Request *	☐ Fee Address Indication Form	☐ Other Enclosure(s) (*please identify below):*
☐ Express Abandonment	☐ Terminal Disclaimer	
☐ Certified Copy of Priority Doc	☐ Power of Attorney and Revocation of Prior Powers	
☐ Response to Incomplete Appln	☐ Change of Correspondence Address	
☐ Response to Missing Parts	*Extension of Term: Pursuant to 37 CFR 1.136, Applicant petitions the Commissioner to extend the time for response for xxxxxx month(s), from to .	
☐ Executed Declaration by Inventor(s)		

CLAIMS					
FOR	Claims Remaining After Amendment	Highest # of Claims Previously Paid For	Extra Claims	RATE	FEE
Total Claims	12	20	0	$ 50.00	$ 0.00
Independent Claims	2	3	0	$200.00	$ 0.00
				Total Fees	$ 0.00

METHOD OF PAYMENT	
☐	Check no. _____ in the amount of $ _____ is enclosed for payment of fees.
■	Charge **$500.00** to Deposit Account No. 50-3533 (Lenovo, Inc.) for payment of fees.
■	Charge any additional fees or credit any overpayment to Deposit Account No. 50-3533 (Lenovo, Inc.).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT	
Attorney Name	Janyce R. Mitchell, Reg. No. 40,095
Signature	*/Janyce R. Mitchell/*Reg. No. 40,095 Janyce R. Mitchell
Date	September 20, 2005

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on **September 20, 2005**

Type or printed name	Jinny Nguyen
Signature	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:

Randall S. SPRINGFIELD et al. Confirmation No: 1231

Serial No: 09/824,595 Group Art Unit: 2135

Filed: April 2, 2001 Examiner: Gyorfi, Thomas A.

For: METHOD AND SYSTEM FOR PROVIDING A TRUSTED FLASH BOOT SOURCE

APPEAL BRIEF

Janyce R. Mitchell
Attorney for Appellants
Lenovo Corporation
Sawyer Law Group LLP

TOPICAL INDEX

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:

Randall S. SPRINGFIELD et al. Confirmation No: 1231

Serial No: 09/824,595 Group Art Unit: 2135

Filed: April 2, 2001 Examiner: Gyorfi, Thomas A.

For: METHOD AND SYSTEM FOR PROVIDING A TRUSTED FLASH BOOT SOURCE

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Appellant herein files an Appeal Brief drafted in accordance with the provisions of 37 C.F.R. § 1.193(b)(1) as follows:

I. REAL PARTY IN INTEREST

Appellant respectfully submits that the above-captioned application is assigned, in its entirety to Lenovo Corporation of Purchase, New York.

II. RELATED APPEALS AND INTERFERENCES

III. STATUS OF CLAIMS

Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, and 12 are pending. Application Serial No. 09/824,595 (the instant application) as originally filed included claims 1-12. In response to an Office Action dated August 5, 2004, claims 1-6 were amended. Claims 1 and 6 were amended to recite that the boot source determines a source of a number of instructions initially executed as a boot source. Claims 1-5 were also amended to remove alphanumeric designation of the steps. In response to a Final Office having a mailing date of March 11, 2005, claims 1 and 6 were amended to delete the recitation added in the previous amendment. Claim 1 was also amended to harmonize claims 1 and 6, adding the limitation that the boot source determining includes writing an identity of the boot source. Claims 2-5 were amended to correct minor errors. Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, and 12 are on appeal and all applied prospective rejections concerning claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, and 12 are herein being appealed.

IV. STATUS OF AMENDMENT

In an Advisory Action having a mailing date of June 14, 2005, the Examiner indicated that the amendment in response to final would be entered upon filing of a Notice of Appeal.

V. SUMMARY OF THE INVENTION

The present invention provides method and system for evaluating a boot source in a computer system having a processor. The method and system comprise determining the boot source used by the processor each time the computer system boots. Thus, the source of the code used in booting the processor is determined. The determination of the boot source may include writing the identity of the boot source rather than the code actually executed, preferably in a first

register. Specification, page 7, lines 1-2. The method and system also include allowing the known boot source to be specified. The known boot source is preferably specified by writing the identity of the known boot source in a second register. Specification, page 7, lines 3-6. As a result, the boot source for the computer is determined (through the identity written) and can be verified using the known boot source. Specification, page 7, lines 6-9. Thus, the boot source can be checked to ensure that a trusted source (the known boot source) has been used. Consequently, a trusted boot source can be provided. Specification, page 7, lines 9-10.

Figure 1 depicts a conventional computer system 10. Specification, page 1, line 6. The conventional computer system 10 includes a FLASH boot source 20, which is typically coupled with the processor 12 through a bridge 16. Specification, page 1, lines 11-12. Thus, the FLASH boot source 20 is used as a boot source for the processor 12 and, once the BIOS has been loaded through booting, the computer system 10 may function. Specification, page 1, lines 12-15. However, it is possible to circumvent the FLASH boot source 20 by placing another boot source at the PCI connector 18. Specification, page 2, lines 3-6. Consequently, the conventional computer system 10 is subject to attack. The computer system 10 could be made secure by a trusted boot source—a boot source that is known and can be verified. For example, the FLASH boot source 20 could be specified as the trusted boot source and the computer system 10 could be precluded from booting from another source. Specification, page 2, lines 11-20. However, this may adversely affect manufacturing, which typically uses a boot source other than the FLASH boot source 20. Specification, page 2, line 20-page 3, line 4.

In contrast, Figure 2 depicts one embodiment of a system 150 in accordance with the present invention for providing a trusted boot source. The system 150 is resides within the computer system 100. The computer system 100 still includes a boot source, shown as the

preferred FLASH boot source, and a processor 112. Figure 2. The system 150 includes two registers 152 and 154. The register 152 is for storing the boot source of the most recent boot, while the register 154 is for storing the known boot source, the boot source from which boots are supposed to be made. Specification, page 6, lines 1-6. By checking the contents of the first register 152 against the contents of the second register 154, it can be ensured that the computer system 100 boots from a known source. Consequently, a trusted boot source can be provided. Specification, page 6, lines 10-11.

Figure 3 depicts a flow chart of one embodiment of a method 200 for providing a trusted boot source. Specification, page 6, lines 12-13. The known boot source is specified, preferably by writing the known boot source to the second register 154, via step 252. Specification, page 6, lines 16-22. In one embodiment, the identity of the FLASH boot source 140 would be written to the second register 154. The identity of the actual boot source used is determined, preferably by writing the identity of the boot source to the first register 152, via step 254. Specification, page 6, line 22-page 7, line 6. For example, as described in the specification, an "identity of the source of the first one hundred instructions" executed is written to the first register 152. Specification, page 7, lines 1-2. The first one hundred instructions themselves are not written. Instead, the identity of their *source* is stored. The identities of the boot source used and the known boot source desired to be used are, therefore, available. The identity of the boot source used (e.g. source of code initially executed) can thus be compared to the known boot source (e.g. the FLASH boot source 140). Consequently, a trusted boot source can be provided. Specification, page 6, lines 13-16.

Figure 4 depicts one embodiment of a method 250 for providing a trusted boot source. Specification, page 7, lines 11-12. The known boot source is specified by writing the identity of

the known boot source to a write-once register such as the second register 154, via step 252. Specification, page 7, lines 15-16. Each time the computer system boots, the identity of the boot source used is written to the first register 152, via step 254. Specification, page 7, lines 21-23. This identity may be the "identity of the source of the first one hundred instructions executed by the computer system 100 . . ." Specification, page 7, lines 21-22. Note that again, the actual instructions themselves are not written.

The identity of the boot source written in step 254 is checked against the known boot source in step 256. Specification, page 8, lines 2-5. Thus, it can be determined whether the boot source used was the known boot source. The computer system may then take appropriate action, via step 258. Specification, page 8, lines 6-10. The appropriate action may include acts such as shutting down if the boot source and known boot source do not match.

Thus, using the system 100 and the methods 200 and/or 250, a trusted boot source may be provided without requiring a significant change in manufacturing of the computer system 100. Specification, page 8, lines 19-21.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

(1) whether claims 1, 4, 6, 7, 9, and 11 are each unpatentable under 35 U.S.C. § 102 as being anticipated by U.S. Patent No. 6,678,833 (Grawrock);

(2) whether claims 2, 3, 5, 10, and 12 are each unpatentable under 35 U.S.C. § 103 as being unpatentable over Grawrock in view of U.S. Patent No. 5,944,821 (Angelo); and

(3) whether claim 8 is unpatentable under 35 U.S.C. § 103 under Grawrock in further view of "VIA's New South Bridge: VT82C686B Supporting UltraATA/100" (Schmid) and "Intel Pentium III i815e Motherboard Shootout" (Sethi).

VII. ARGUMENTS

A. Summary of the Applied Rejections

In the Final Office Action, dated March 11, 2005, the Examiner rejected claims 1, 4, 6, 7, 9, and 11 under 35 U.S.C. § 102 as being anticipated by Grawrock. In so doing, the Examiner cited Grawrock, col. 3, lines 62-67 and col. 4 lines 10-18 and 25-30. The Examiner particularly cited col. 4, lines 25-30 as describing writing an identity of a trusted boot source. In particular, the Examiner stated that:

> **Grawrock discloses that the boot block memory contains boot block code (i.e. a number of instructions) that are executed at the start of the initialization process (col. 3, lines 39-44). Further, the determination of the boot source occurs during the initialization process, implying that some number of instructions have already been executed by the boot source at the time of the determination (col. 4, lines 25-30).**

The Examiner also rejected claims 2, 3, 5, 10, and 12 under 35 U.S.C. § 103 as being unpatentable over Grawrock in view of Angelo. In so doing, the Examiner acknowledged that Grawrock does not explicitly teach that the boot source is a flash boot source. The Examiner also stated that "Angelo teaches a computer system having a flash ROM containing the BIOS information."

The Examiner also rejected claim 8 under 35 U.S.C. § 103 under Grawrock in further view of Schmid and Sethi. The Examiner indicated that Grawrock discloses that "the bridge is an ICH, which is known in the art as a south bridge. . ." The Examiner also indicated that an ICH is identical to a south bridge as shown in Schmid and Sethi.

Appellant respectfully requests that the Board reverse the Examiner's final rejection of claims 1, 4, 6, 7, 9, and 11 under 35 U.S.C. § 102; claims 2, 3, 5, 10, and 12 under 35 U.S.C. § 103; and claim 8 under 35 U.S.C. § 103.

B. The Cited Prior Art

Grawrock describes a system which provides a boot block *identifier* from the boot block memory unit, either the first time the computer system starts up or each time the system starts up. Grawrock, col. 3, lines 57-67. In particular, Grawrock states that the:

> boot block memory unit loads and records its boot block identifier into the memory . . . Next, the boot block memory unit locates and loads the BIOS for execution . . . The BIOS (or a representation thereof) is loaded to the TPM and a BIOS identifier is recorded . . .

Grawrock, col. 4, lines 25-30. Thus, Grawrock does state that a BIOS identifier and the boot block identifier are recorded. However, the boot block identifier is a hash of "boot information." Grawrock, col. 3, lines 57-61. Grawrock further states that the "boot information" is basically an image or series of sub-images that collectively *represent* the boot block code. Grawrock, col. 3, lines 45-50. Thus, the boot information corresponds to the boot code itself, rather than to an identity of the boot source. In response to challenges, a digital signature is provided. Grawrock, col. 4, lines 10-16. This digital signature is a combination of the boot block identifier, keying material, certificates, and other similar information. Grawrock, col. 4, lines 17-18. Consequently, Grawrock describes providing a boot block identifier and a digital signature incorporating the boot block identifier that are both based on a representation of the boot block code actually used rather than on the identity of the boot source.

Angelo describes a system for secure registration and integrity assessment of software. Angelo, Abstract. Consequently, Angelo does describe hashing. Angelo, Abstract. In addition, as cited by the Examiner, Angelo does state that BIOS information for the computer system may be contained in a flash Rom. Angelo, col. 7, lines 30-34. However, Angelo is more concerned with validating individual programs for execution, and so discusses providing the secure hash table for

indicating the programs that are validated. Angelo, col. 4, lines 41-54. Thus, execution of the secured programs may be monitored and controlled. Angelo, col. 4, line 55-col. 5, line 5.

Schmid and Sethi describe a south bridge. For example, Schmid describes products incorporating a south bridge. Schmid, second full paragraph. Similarly Sethi describes a number of semiconductor devices incorporating north bridges and/or south bridges.

C. Claims 1, 4, 6, 7, 9, and 11 Are Not Unpatentable Under 35 U.S.C. § 102.

Appellant respectfully submits that the applied rejections of claims 1, 4, 6, 7, 9, and 11 under 35 U.S.C. § 102 are without merit as the Examiner has completely failed to explain why Grawrock teaches or suggests the method and system recited in claims 1 and 6.

Independent claims 1 and 6 recite a method and system, respectively, for evaluating a boot source in a computer system. In particular, Grawrock fails to teach or suggest "determining the boot source used by the processor each time the computer system boots, the boot source determining further including writing an identity of the boot source" in conjunction with allowing the boot source to be specified once as a known boot source, as recited in claim 1. Similarly, claim 6 recites a system for evaluating a boot source in a computer system including "a first register for storing an identity of the boot source used by the processor each time the computer system boots. . . and a second register for allowing the boot source to be specified once as a known boot source."

Using the method and system recited in claims 1 and 6, respectively, a boot source can be evaluated. In particular, the identity of the boot source used is stored. As described in the specification, the identity of the boot source corresponds *not* to the actual code booted, but to

another feature, that identifies the **source** of the boot code. Specification, page 7, lines 1-2 and 21-23. See also, specification, page 7, lines 4-5 (indicating the identity of the FLASH boot source 140 is written, not the contents of the FLASH boot source). By comparing the identity of the boot source to the known boot source, the source of the instructions that are actually executed can be provided and independently verified. Specification, page 8, lines 13-15. Consequently, a trusted boot source can be reliably provided. Specification, page 8, lines 15-16. This can be accomplished without requiring a significant change in manufacturing of the computer system. Specification, page 8, lines 19-21.

Grawrock fails to teach or suggest writing an identity of the boot source to a register or any other location. As discussed above, Grawrock describes a system which provides a boot block *identifier* that is not an identity of the boot *source*. Instead, the boot block identifier of Grawrock is based on the code actually used during booting. As described above, the boot block identifier of Grawrock is based (is a hash of) boot information. This boot information represents the boot block code. The boot information and, therefore, the boot block identifier, corresponds to the boot code itself. Because the boot block identifier is based on the boot code itself, the boot block identifier of Grawrock merely corresponds to the contents of (instructions in) the boot source. The boot block identifier of Grawrock, therefore, does not correspond to the identity of the boot source. Grawrock thus fails to teach or suggest the recited writing of the boot block identity. Thus, Grawrock fails to teach or suggest a method and system recited in claims 1 and 6. Consequently, Appellant respectfully submits that claims 1 and 6 are allowable over the cited references.

Clams 4 and claims 7, 9, and 11 depend upon independent claims 1 and 6, respectively. Consequently, the arguments herein apply with full force to claims 4, 7, 9, and 11. Accordingly, Appellant respectfully submits that claims 4, 7, 8, and 11 are allowable over the cited references.

Accordingly Appellant respectfully requests that the Board reverse the final rejection of claims 1, 4, 6, 7, 9, and 11 under 35 U.S.C. § 102.

D. Claims 2, 3, 5, 10, and 12 Are Not Unpatentable Under 35 U.S.C. § 103

Appellant respectfully submits that the applied rejections of claims 2, 3, 5, 10 and 12 under 35 U.S.C. § 103 are without merit as the Examiner has completely failed to explain why Grawrock in view of Angelo teaches or suggests the methods and systems recited in claims 2, 3, and 5 and claims 10 and 12, respectively.

Claims 2, 3, and 5 depend upon independent claim 1. Claims 10 and 12 depend upon independent claim 6. Consequently, the arguments herein with respect to Grawrock apply with full force to claims 2, 3, 5, 10, and 12. In particular, Grawrock fails to teach or suggest writing an identity of the boot source.

Angelo fails to remedy the defects of Grawrock. Angelo describes a system for secure registration and assessment of software and, therefore, does describe hashing. Angelo does state that BIOS information for the computer system may be contained in a flash ROM. Angelo, col. 7, lines 30-34. However, Applicant has found no mention in Angelo of writing the identity of the boot block, for example to a register. Consequently, any combination of Grawrock and Angelo would also be devoid of this feature. Stated differently, if the system of Grawrock were combined with that of Angelo, the combination might use the flash ROM as a boot source. Using the teachings of Grawrock, the contents of the flash ROM may be used to form the boot identifier of Grawrock. However, the combination would still not write the *identity* of the flash ROM to determine the boot source. Consequently, Grawrock in view of Angelo fails to teach or suggest the methods and

systems recited in claims 2, 3, 5, 10, and 12. Accordingly, Appellant respectfully submits that claims 2, 3, 5, 10, and 12 are allowable over the cited references.

Accordingly Appellant respectfully requests that the Board reverse the final rejection of claims 2, 3, 5, 10, and 12 under 35 U.S.C. § 103.

E. Claim 8 Is Not Unpatentable Under 35 U.S.C. § 103

Appellant respectfully submits that the applied rejections of claim 8 under 35 U.S.C. § 103 is without merit as the Examiner has completely failed to explain why Grawrock in view of Schmid and/or Sethi teaches or suggests the system recited in claim 8.

Claim 8 depends upon independent claim 6. Consequently, the arguments herein with respect to Grawrock apply with full force to claim 8. In particular, Grawrock fails to teach or suggest writing an identity of the boot source.

Schmid and Sethi fail to remedy the defects of Grawrock. Schmid and Sethi both describe semiconductor devices including bridges. However, Applicant has found no mention in Schmid or Sethi of writing the identity of the boot block, for example to a register. Consequently, any combination of Grawrock and Schmid and/or Sethi would also be devoid of this feature. Stated differently, if the system of Grawrock were combined with that of Schmid and/or Sethi, the combination might use south and/or north bridges. Using the teachings of Grawrock, the contents of the flash ROM may be used to form the boot identifier of Grawrock. However, the combination would still not write the *identity* of the flash ROM to determine the boot source. Consequently, Grawrock in view of Schmid and/or Sethi fails to teach or suggest the methods and systems recited in claim 8. Accordingly, Appellant respectfully submits that claim 8 is allowable over the cited references.

Accordingly Appellant respectfully requests that the Board reverse the final rejection of claim 8 under 35 U.S.C. § 103.

F. Summary of Arguments

For all the foregoing reasons, it is respectfully submitted that Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, and 12 (all the claims presently in the application) are patentable for defining subject matter which would not have been obvious under 35 U.S.C. § 103 or anticipated under 35 U.S.C. § 102(e) at the time the subject matter was invented. Thus, Appellant respectfully requests that the Board reverse the rejection of all the appealed Claims and find each of these Claims allowable.

Note: For convenience of detachment without disturbing the integrity of the remainder of pages of this Appeal Brief, Appellant's "APPENDIX" section is contained on separate sheets following the signatory portion of this Appeal Brief.

Authorization for payment of the required Brief fee is contained in the transmittal letter for this Brief. Please charge any fee that may be necessary for the continued pendency of this application to Deposit Account No. 50-3533 (Lenovo, Inc.).

Very truly yours,

September 20, 2005
Date

*/Janyce R. Mitchell/*Reg. No. 40,095
Janyce R. Mitchell
Attorney for Appellants
Reg. No. 40,095
(650) 493-4540

VIII. CLAIMS APPENDIX

1. A method for evaluating a boot source in a computer system having a processor comprising:

determining the boot source used by the processor each time the computer system boots, the boot source determining further including writing an identity of the boot source; and

allowing the boot source to be specified once as a known boot source.

2. The method of claim 1 wherein the known boot source allowing step further includes:

specifying that the known boot source to be a FLASH boot source.

3. The method of claim 2 wherein the specifying step further includes:

writing the identity of the FLASH boot source in a write-once register which identifies the boot source for future boots.

4. The method of claim 1 wherein the determining step further includes:

writing the identity of the boot source in a register each time the computer system boots.

5. The method of claim 1 further comprising:

checking the boot source determined to ensure that the boot source is the known boot source.

6 A system for evaluating a boot source in a computer system having a processor coupled with a boot source, the system comprising:

a first register for storing an identity of the boot source used by the processor each time the computer system boots; and

a second register for allowing the boot source to be specified once as a known boot source.

7. The system of claim 6 wherein the computer system includes a bridge coupling the processor with the boot source and wherein the first register and the second register are located in the bridge.

8. The system of claim 7 wherein the bridge is a south bridge.

9. The system of claim 6 wherein the known boot source is written only once to the second register.

10. The system of claim 9 wherein the known boot source is a FLASH boot source.

11. The system of claim 6 wherein the identity of the boot source is written to the first register each time the computer system boots.

12. The system of claim 6 wherein the processor is capable of checking the boot source stored in the first register to ensure that the boot source is the known boot source.

IX. EVIDENCE APPENDIX

X. RELATED PROCEEDINGS APPENDIX